UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,226	10/04/2001	Vadim Lander	063170.6963(20000430)	4394

5073 7590 04/11/2007

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/11/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/11/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mike.furr@bakerbotts.com
ptomail1@bakerbotts.com

Office Action Summary	**Application No.** 09/972,226	**Applicant(s)** LANDER, VADIM	
	Examiner Eleni A. Shiferaw	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 22 January 2007.

2a)☒ This action is **FINAL**.   2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-30 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-30 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to amended claim 12 and original claims 1-11, and 13-30 filed 01/22/2007 have been fully considered but they are not persuasive.

Regarding argument reference Steele failure to disclose "retrieving, from the repository of user information, a unique universal user identifier representing said user upon locating said information of said user" as recited in claim 1, remark page 8 par. 4-page 9 par. 1, is not persuasive because Steele et al. discloses a method of single sign-on for access to central data repository (abstract) and a user/consumer requesting a creation of an information account 110 (col. 16 lines 14-19), and a ticket (col. 9 lines 56-57) by transmitting consumer data to host 108(col. 16 lines 14-19) and host server 108 creating and providing **authentication information** (col. 16 lines 64-67) **that is *associated with the received consumer data* and the vendor** (col. 8 lines 2-3). Authentication information are password and/or username, key, certificate, (col. 7 lines 36-40 and col. 8 lines 4-6), and **ticket**, that refers to a temporary authorization for at least partial access to a consumer's information account 110, and that is associated with a data structure that correlates tickets with a set of consumer-defined attributes (consumer-defined attributes are number of times that the user password may be used to access info. account 110, consumer ticket expiration time, number of identifiers which may be used to ensure that the party using the ticket is in fact authorized to do so) (col. 9 lines 56-col. 10 lines 7). Ticket is consumer authentication information (col. 13 lines 45-52) that is associated with and/or based on consumer data (col. 8 lines 2-3) and stored in the central data repository 102 (see fig. 4 element 402; consumer authentication information), and ticket is retrieved from central repository and consumer is authenticated and client browser is directed to another web page data file of vendor server by including the retrieved ticket as a parameter in the URL, based on consumer authentication result in host server 108 (see col. 10 lines 8-18 and col. 8 lines 46-67). Ticket generated by host 108 in response to user request to access the vendor server is "GLOBALLY UNIQUE IDENTIFIER" (GUID). A GUID may comprise a unique number that is computed by adding the time and data to a network adapter's internal serial number or by any other suitable technique but the ticket identifies each ticket requester consumer and/or the ticket is generated based on consumer information data (col. 8 lines 2-3).

Regarding argument claims 12, 18, 23, and 28 should be patentable for at least same reasons as discussed/argued above... remark page 9 par. 4, argument is not persuasive because reasons argued above is not claimed for claims 12, 18, 23, and 28 and/or "*retrieving, from the repository of user information*, a unique universal user identifier representing said user upon locating said information of said user" recited in claim 1 is not the same as "a unique universal user identifier corresponding to a user" claim 12, "each of said unique universal user identifiers being unique to a user." Claim 18, "each unique universal user identifiers being unique to a user" claim 23, and "a unique universal user identifier representing said user" claim 28. Moreover, ticket if Steele et al. is GUID (see col. 10 lines 19-24).

The rejection(s) for claims 1-30 are respectfully maintained.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-30 are rejected under 35 U.S.C. 102(e) as being anticipated by Steele et al. USPN 7,016,875 B1.

Regarding claim 1, Steele et al. discloses a method for authenticating and authorizing a user of an electronic device in communication with a network (fig. 1 and col. 2 lines 43-col. 3 lines 39), comprising:

receiving a user request from a user of an electronic device in communication with a network (fig. 11 element 1102, 1104 and 1106; *client device, consumer authentication information, and host server repository table*);

searching for information relating to said user in a repository of user information, said searching based at least partially on said user request and a login identity supplied by said user (col. 8 lines 46-col. 9 lines 2 and col. 23 lines 53-col. 24 lines 62);

retrieving, from the repository of user information, a unique universal user identifier representing said user upon locating said information of said user (fig. 11 & 4, col. 8 lines 60-col. 9 lines 2, and col. 9 lines 53-col. 10 lines 31 and col. 25 lines 24-col. 26 lines 44);

storing at least said unique universal user identifier in a data packet (col. 8 lines 60-col. 9 lines 2, and col. 23 lines 10-col. 24 lines 62);

sending said data packet to a storage device such that said data packet is transmittable to electronic devices in communication with said network when said user attempts to access a resource within said network (col. 8 lines 67-col. 9 lines 12 and col. 25 lines 46-67); and

retrieving an authorization datum associated with said user, based at least partially on said unique universal user identifier, from said resource (col. 9 lines 13-col. 10 lines 43).

Regarding claim 12, Steele et al. discloses a method for accessing a plurality of resources (fig. 8 elements 802Y and 802Z) having different authorization requirements (abstract), comprising:

accessing, via an electronic device, a network comprising a plurality of resources (fig. 1);

providing identifying data to said network (col. 23 lines 10-67);

retrieving, in response to the identifying data, a unique universal user identifier corresponding to said user from a repository of unique universal user identifiers (fig. 11 & 4, col. 8 lines 60-col. 9 lines 2, and col. 9 lines 53-col. 10 lines 31 and col. 25 lines 24-col. 26 lines 44);

storing said unique universal user identifier on a storage device, said unique universal user identifier indicating said user is authenticated (col. 24 lines 2-col. 25 lines 63); and

accessing one of said plurality of resources, wherein said unique universal user identifier is transmitted to said one of said plurality of resources to identify said user such that said user can access authorized resources without providing additional identifying information and said user is denied access to unauthorized resources (col. 25 lines 5-col. 26 lines 44).

Regarding claim 18, Steele et al. discloses a method of user authentication and authorization (fig. 11), comprising:

accessing a repository containing a plurality of unique universal user identifiers, each of said unique universal user identifiers being unique to a user (fig. 1 element 102, and col. 9 lines 3-col. 10 lines 44);

retrieving one of said unique universal user identifiers from said repository (fig. 11 & 4, col. 8 lines 60-col. 9 lines 2, and col. 9 lines 53-col. 10 lines 31 and col. 25 lines 24-col. 26 lines 44);

storing said unique universal user identifier in a data packet readable by an electronic device (col. 8 lines 60-col. 9 lines 2, and col. 23 lines 10-col. 24 lines 62);

transmitting said data packet to a storage device coupled to said electronic device (col. 8 lines 67-col. 9 lines 12 and col. 25 lines 46-67); and

making said data packet available to a resource configured within an enterprise network to authorize said user (col. 9 lines 13-col. 10 lines 43 and col. 25 lines 24-63).

Regarding claim 23, Steele et al. discloses a system for user authentication and authorization, comprising:

a repository containing a plurality of unique universal user identifiers, each unique universal user identifier being unique to a user (fig. 4, fig. 1 element 102, and col. 9 lines 3-col. 10 lines 44);

a first software tool operable to receive user login information, access said repository, retrieve a unique universal user identifier relating to said user, and transmit said unique universal user identifier to an electronic storage device suitable for storing said unique universal user identifier in a data packet for transmission to resources within a network (fig. 11, col. 8 lines 60-col. 9 lines 2, and col. 9 lines 53-col. 10 lines 31 and col. 25 lines 24-col. 26 lines 44); and

a second software tool suitable for receiving said data packet and locating authorization datum of said user (col. 9 lines 13-col. 10 lines 43 and col. 25 lines 24-63).

Regarding claim 28, Steele et al. discloses a computer-readable medium encoded with logic operable, when executed on a computer processor, to perform the steps comprising:

receiving a user request from a user of an electronic device (fig. 11 element 1102, 1104 and 1106);

searching for a user credential corresponding to said user in an authentication database (col. 8 lines 46-col. 9 lines 2 and col. 23 lines 53-col. 24 lines 62);

locating said user credential in said authentication database (col. 8 lines 46-col. 9 lines 2 and col. 23 lines 53-col. 24 lines 62);

retrieving a unique universal user identifier representing said user upon locating said user credential (fig. 11 & 4, col. 8 lines 60-col. 9 lines 2, and col. 9 lines 53-col. 10 lines 31 and col. 25 lines 24-col. 26 lines 44);

packaging said unique universal user identifier in a data packet (col. 8 lines 67-col. 9 lines 12 and col. 25 lines 46-67); and

transmitting said data packet to said electronic device such that said data packet is transmittable to electronic devices in communication with a network when said user attempts to access a resource within said network such that said user can access authorized resources without providing additional identifying information (col. 15 lines 1-51).

As per claim 2, Steele et al. discloses the method, wherein receiving a user request comprises receiving a login name from said user (col. 8 lines 1-24).

As per claim 3, Steele et al. discloses the method further comprising:

registering said user with said network (fig. 2);

generating said user identifier relating to said user (col. 9 lines 2-col. 10 lines 44);

inserting said user identifier in said repository of user information (col. 23 lines 62-col. 24 lines 62); and

populating a plurality of repositories containing authorization data with said user identifier (col. 25 lines 24-63).

As per claim 4, Steele et al. discloses the method further comprising receiving a security identity from said user (col. 9 lines 2-65).

As per claim 5, Steele et al. discloses the method further comprising receiving a digital certificate from said user (col. 8 lines 1-24).

As per claim 6, Steele et al. discloses the method further comprising indicating a result to said user regarding permitted access to said network (col. 8 lines 60-col. 9 lines 2).

As per claim 7, Steele et al. discloses the method further comprising requesting a user credential of said user (col. 24 lines 38-lines 62).

As per claim 8, Steele et al. discloses the method, wherein sending said data packet to a storage device comprises sending said data packet to a user electronic device supporting said storage device (col. 15 lines 1-51).

As per claim 9, Steele et al. discloses the method further comprising storing information in addition to said unique universal user identifier in said data packet (col. 8 lines 60-col. 9 lines 2, and col. 23 lines 10-col. 24 lines 62).

As per claim 10, Steele et al. discloses the method, wherein sending said data packet to a storage device comprises transmitting a cookie to said user electronic device enabling an identity of said user to be automatically recognized when said cookie is transmitted to said resource within said network (col. 2 lines 42-60).

As per claim 11, Steele et al. discloses the method further comprising encrypting said data packet (col. 9 lines 9-12).

As per claim 13, Steele et al. discloses the method, further comprising providing a key to retrieve an authorization datum associated with one of said plurality of unique user identifiers matching said unique universal user identifier from one of said plurality of resources (col. 10 lines 19-30). As per claim 17, Steele et al. discloses the method, wherein providing identifying data to said network comprises providing a digital certificate (col. 10 lines 19-30).

Regarding claim 14, Steele et al. discloses the method, further comprising:

registering said user with said network (fig. 2);

generating said unique universal user identifier for said user (fig. 4 and col. 9 lines 2-col. 10 lines 44); and

inserting said unique universal user identifier in at least one of said plurality of user identifiers (col. 23 lines 62-col. 24 lines 62).

As per claim 15, Steele et al. discloses the method, wherein providing identifying data to said network comprises supplying at least one of a login name, a password, and a digital certificate (col. 8 lines 1-24).

As per claim 16, Steele et al. discloses the method, wherein providing identifying data to said network comprises providing user credentials (col. 8 lines 1-24).

As per claim 17, Steele et al. discloses the method, wherein providing identifying data to said network comprises providing a digital certificate (col. 8 lines 1-24).

As per claim 19, Steele et al. discloses the method, wherein storing said unique universal user identifier comprises packaging said unique universal user identifier in a cookie suitable for storage on at least one of a user electronic device and a user proxy electronic device (fig. 4, and col. 9 lines 42-col. 10 lines 44).

As per claim 20, Steele et al. discloses the method further comprising employing a software program to access a network reading said storage device (col. 6 lines 11-29).

As per claim 21, Steele et al. discloses the method further comprising employing a web browser employed to access a network reading said storage device (col. 2 lines 43-60 and fig. 9).

As per claim 22, Steele et al. discloses the method further comprising:

delivering said data packet to said resource configured within said enterprise network (col. 9 lines 20-24);

extracting said unique universal user identifier from said data packet (col. 25 lines 24-col. 26 lines 44);

accessing a repository containing a plurality of user entitlement data (col. 25 lines 24-col. 26 lines 44); and

retrieving a user-specific entitlement from said repository containing said plurality of user entitlement data using said unique universal user identifier to locate said user-specific entitlement (col. 25 lines 24-col. 26 lines 44).

As per claim 24, Steele et al. discloses the system, wherein said electronic storage device is readable by a software program suitable for accessing said network (fig. 10 element 102).

As per claim 25, Steele et al. discloses the system, wherein said software program is a web browser (fig. 9).

As per claim 26, Steele et al. discloses the system, wherein said electronic storage device is a resource configured within said network (fig. 8).

As per claim 27, Steele et al. discloses the system, further comprising a repository containing authorization data, said repository containing authentication data accessible using said unique universal user identifier as a key to retrieve a user-specific entitlement associated with said user (fig. 2-4).

As per claim 29, Steele et al. teaches the computer readable medium, further operable, when executed on a computer processor, to perform the steps comprising:

transmitting said data packet to said resource within said network (col. 9 lines 20-24);

accessing a repository containing a plurality of user identifiers using said packaged unique universal user identifier in a search operation (col. 25 lines 24-col. 26 lines 44); and retrieving a user-specific entitlement from said repository containing a plurality of unique universal user identifiers, said user-specific entitlement associated with said packaged unique universal identifier (col. 25 lines 24-col. 26 lines 44).

As per claim 30, Steele et al. teaches the computer readable medium, further operable, when executed on a computer processor, to perform the step of requesting a user credential (fig. 1 element 108).

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 6,836,799 B1: ***Philyaw et al. discloses a user providing information like serial number, name, address, job, income level, general family history, demographic information and more and generating unique identification/unique ID based on user information provided i.e. generating a unique universal identifier is very well known in the art.***

For more prior art of record see form PTO 892 attached.

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

April 4, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

4/4/07